IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

LINDA NEWTON, individually and on behalf of all others similarly situated,	)	CASE NO.
Plaintiff,	)	**COMPLAINT -- CLASS ACTION**
v.	)	
WAWA, INC., a New Jersey corporation,	)	
Defendant.	)	**JURY TRIAL DEMANDED**

Plaintiff Linda Newton ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Defendant Wawa, Inc. ("Wawa" or "Defendant") based on personal knowledge as to her own experiences and on information and belief from the investigation of counsel:

INTRODUCTION

1. With this action Plaintiff seeks to hold Wawa responsible for the harm it caused her and thousands of other customers in the massive data breach that took place between March 4, 2019 and December 12, 2019 (the "Data Breach").

2. In the Data Breach, cyber criminals were able to infiltrate Wawa's computer systems, migrate to Wawa's payment card environment, and install malicious software on the point of sale (POS) systems at potentially all of Wawa's 850 locations, including convenience stores and gas stations. Once the malicious software was successfully installed on Wawa's POS system, the cyber criminals were able to steal the financial data of millions of unsuspecting customers for most of a year without being disturbed by Wawa. Wawa's reckless failure to meet industry standards of cyber security allowed this to happen.

3. Because of Wawa's inadequate and negligent security measures and failure to adequately monitor its payment systems, cyber criminals were able to steal vast amounts of sensitive personal information, including credit card and debit card numbers, expiration dates, cardholder names, internal verification codes, and other card information (collectively, "Payment Data").

4. As a result of the Data Breach, millions of consumers have reportedly had their sensitive credit and debit card information exposed to fraudsters resulting from purchases made at Wawa locations.

5. Wawa first announced the breach on December 19, 2019, in a press release, stating:

> Wawa is notifying potentially impacted individuals about a data security incident that affected customer payment card information used at potentially all Wawa locations during a specific timeframe. Based on the investigation to date, the information is limited to payment card information, including debit and credit card numbers, expiration dates and cardholder names, but does not include PIN numbers or CVV2 numbers.[1]

6. As alleged below, Wawa's failure to implement adequate data security measures for this sensitive customer information directly and proximately caused injuries to Plaintiff and the class.

7. The Data Breach was the inevitable result of Wawa's inadequate and negligent data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and despite the fact that these types of data breaches were and are occurring throughout the restaurant and retail industries, Wawa failed to ensure that it maintained adequate data security measures causing customer Payment Data to be stolen.

[1] "Wawa Notifies Customers of Data Security Incident," WAWA (Dec. 19, 2019).

8. As a direct and proximate consequence of Wawa's conduct and data security shortcomings, a massive amount of customer information was stolen from Wawa and placed into the hands of criminals. Victims of the Data Breach have had their Payment Data compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise been injured.

9. Moreover, Plaintiff and class members have been forced to spend significant time associated with, among other things, closing out and opening new credit or debit card accounts, ordering replacement cards, obtaining fraud monitoring services, losing access to cash flow and credit lines, monitoring credit reports and accounts, and/or other losses resulting from the unauthorized use of their cards or accounts.

10. Plaintiff and class members seek to recover damages caused by Wawa's negligence, negligence *per se*, breach of contract, and violations of state consumer protection statutes. Additionally, Plaintiff seeks declaratory and injunctive relief as a result of the conduct of Wawa discussed herein.

PARTIES

Plaintiff Linda Newton

11. Plaintiff Linda Newton is a citizen of Pennsylvania, residing in Lehigh County.

12. Plaintiff Newton has been a frequent Wawa customer, shopping at multiple Wawa locations several times a month, ever month, for years. To give just three examples, she used her debit card to make purchases at Wawa locations on June 5, 2019, November 27, 2019, and November 26, 2019.

13. There are twenty Wawa gas station and convenience store locations within a thirty-minute drive of Plaintiff's home in Center Valley, Pennsylvania.

14. Between March 4 and December 12, 2019, Plaintiff Newton shopped at many of these locations, and used her debit card to make purchases. For example, she made purchases at Wawa locations in Quakertown and Allentown, Pennsylvania, and Flemington and Phillipsburg, New Jersey during the Breach Period.

15. She expected that Wawa would use industry best practices to protect her Payment Data.

16. On December 22, 2019, Plaintiff Newton received a "low balance alert" from her bank.

17. She logged into her account and found that someone had used her card to make fraudulent purchases, including a purchase for gas at a Wawa location in Phillipsburg, New Jersey.

18. On December 23, Plaintiff Newton called and spoke with the manager at the New Jersey location, who told her about the Data Breach. She was on the phone for over half an hour with Wawa trying to determine how this occurred.

19. Newton then drove to the Quakertown Wawa location to speak with the manager. The manager there was unable to process a refund for the fraudulent purchase.

20. Also on December 23, someone used Plaintiff Newton's bank account and made a fraudulent purchase of $51.94 at a Walmart.com. This fraudulent purchase overdrew her checking account causing her to have a negative account balance.

21. Plaintiff Newton called her bank to report the fraud, and her debit card was canceled, leaving her without means to make purchases.

22. Plaintiff Newton has been harmed by this data breach, including the fraudulent charges, lost time responding to it, the time she spent driving to the Quakertown location, as well as overpayment for goods and fuel at Wawa locations based on an implied part of the bargain that

Wawa would comply with reasonable payment card security standards. She also lost the time value of the money stolen from her bank account, and has faced hardship from being left without her debit card.

23. Because of the saturation of Wawa locations in the gas station market near her home, Newton anticipates having to purchase fuel and other items from Wawa in the future. She is therefore very concerned that Wawa make significant and serious improvements to its data security, and that these changes be Court ordered and enforceable.

Defendant Wawa, Inc.

24. Defendant Wawa, Inc. is one of the largest privately owned corporations in America. It is incorporated in New Jersey and maintains its principal place of business at 260 West Baltimore Pike, Wawa, Pennsylvania 19063.

25. Wawa is a sophisticated business that represents itself as being a leader in the industry and being "fully committed to data security."

26. It operates a chain of gas stations, convenience stores, and related businesses, including over 850 locations in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Washington D.C., and Florida.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Wawa. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

28. This Court has personal jurisdiction over Defendant, as Wawa's principal place of business is in Pennsylvania and a substantial part of the events and/or omissions giving rise to the claims occurred within this State and District. Venue is also proper in this District under 28 U.S.C. § 1391(a)(2).

FACTUAL ALLEGATIONS

The Data Breach

29. On December 19, 2019, Wawa notified the public in "An Open Letter from Wawa CEO Chris Gheysens to Our Customers" posted on its corporate website that it had suffered a data breach that compromised customers' sensitive Payment Data. The notice provides the following:

> Based on our investigation to date, we understand that at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. Although the dates may vary and some Wawa locations may not have been affected at all, this malware was present on most store systems by approximately April 22, 2019. Our information security team identified this malware on December 10, 2019, and by December 12, 2019, they had blocked and contained this malware.[2]

30. The Notice further states the following about what information was involved: "Based on our investigation to date, this malware affected payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019 and ending on December 12, 2019."

31. It is apparent from the little information that Wawa has published to date that it did not use the latest card encryption technology.

[2] "Wawa Data Security – Updates & Customer Resources," WAWA (Dec. 19, 2019), https://www.wawa.com/alerts/data-security.

32. Point-to-point encryption technology in POS systems exists that is designed to defeat card-skimming malware. If Wawa had used this technology, the data breach would not have happened.

Industry Standards and Governmental Guidance for Protection of Payment Data

33. It is well known that sensitive Payment Data is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. At least 11 consumer companies reported data breaches in the last year. Many of them were caused by flaws in payment systems either online or in stores."[3]

34. Despite the known risk of a data breach and the widespread publicity and industry alerts regarding the other notable data breaches, Wawa failed to take reasonable steps to adequately protect its computer systems from being breached, and then failed to detect the Data Breach for several months.

35. Wawa is, and at all relevant times has been, aware that the Payment Data it maintains as a result of purchases made at its locations is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. Indeed, it used heightened data security technology at its grocery store, pharmacy, and convenience store locations, but not at the locations that were impacted by the Data Breach.

36. Wawa recognizes the importance of adequately safeguarding its customers' sensitive Payment Data. On its website, Wawa states: "Protecting your privacy is important to Wawa." It's online Privacy Policy, last updated in June 2019—during the heart of the Data

[3]Dennis Green & Mary Hanbury, "If you bought anything from these 11 companies in the last year, your data may have been stolen," BUSINESS INSIDER (Aug. 15, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

Breach—states that Wawa is "fully committed to data security."[4]

37. Wawa is thus aware of the importance of safeguarding its customers' Payment Data from the foreseeable consequences that would occur if its data security systems were breached.

38. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

39. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Wawa to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

40. The twelve requirements of the PCI DSS are:

1. Install and maintain a firewall configuration to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;
3. Protect stored cardholder data;
4. Encrypt transmission of cardholder data across open, public networks;
5. Protect all systems against malware and regularly update anti-virus software or programs;
6. Develop and maintain secure systems and applications;
7. Restrict access to cardholder data by business need to know;
8. Identify and authenticate access to system components;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes; and
12. Maintain a policy that addresses information security for all personnel.[5]

[4]"Privacy Policy," WAWA (Last Updated June 24, 2019), https://www.wawa.com/privacy.
[5]Payment Card International (PCI) Data Security Standard, "Requirements and Security Assessment Procedures,

41. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

42. Wawa was at all times fully aware of its data protection obligations in light of its participation in the payment card processing networks and the stores daily collection and transmission of thousands of sets of Payment Data.

43. Because Wawa accepted payment cards containing sensitive financial information, it knew that its customers were entitled to and did in fact rely on it to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

44. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3d Cir. 2015); *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

45. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be

Version 3.2.1," (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1574069601944.

trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

46. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[6]

47. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses in regard to their data security obligations.

48. As noted above, Wawa was aware of the need to have adequate data security systems in place.

49. Despite this, Wawa failed to upgrade and maintain its data security systems in a meaningful way so as to prevent data breaches. Wawa's cyber security runs afoul of industry best practices and standards. More specifically, the security practices in place at Wawa are in stark contrast and directly conflict with the PCI DSS core security standards.

50. Had Wawa maintained its information technology systems ("IT systems"), adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach.

51. As a result of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented restaurant and retail (and other) data breaches, Wawa was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

52. Wawa was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used recently to infiltrate large

[6]FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited November 8, 2019).

retailers such as, *inter alia*, Target, GameStop, Chipotle, Jason's Deli, Chili's Bar & Grill, Hy-Vee, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Wawa was aware that malware is a real threat and is a primary tool of infiltration used by hackers.

53. In addition to the publicly announced data breaches described above, Wawa knew or should have known of additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[7]

54. Likewise, in October 2014—over six years ago—then-President Barak Obama signed an executive order and started the BuySecure Initiative with the goal of improving data security in the payment card industry to combat "America's fastest-growing crime."[8] Many of the enhanced security measures advocated in the BuySecure Initiative over half a decade ago were never implemented by Wawa.

55. Despite the fact that Wawa was on notice of the very real possibility of consumer data theft associated with its security practices and that Wawa knew or should have known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols, and permitted massive malware intrusions to occur for months on end.

56. And this despite passing along the costs of maintaining up-to-date POS systems onto its customers.

57. Any merchant that accepts payment cards, such as Wawa, is quite used to the idea

[7]*See* U.S. COMPUTER EMERGENCY READINESS TEAM, "Alert (TA14-212A): Backoff Point-of-Sale Malware," (July 31, 2014) (revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A.
[8]"FACT SHEET: Safeguarding Consumers' Financial Security," THE WHITE HOUSE: OFFICE OF THE PRESS SECRETARY (Oct. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/fact-sheet-safeguarding-consumers-financial-security.

of passing along costs to consumers. This is because for the privilege of accepting payment cards for sales, the merchant must pay transaction and account fees.[9]

58. One of the costs of accepting payment cards is the additional security that is required. And businesses don't offer this added security to their consumers for free—it too is built into the price. Yet here, Wawa customers did not get what they paid for.

59. Wawa at all times relevant to this action had a duty to Plaintiff and members of the class to: (a) properly secure Payment Data submitted to or collected at Wawa locations and on Wawa's internal networks; (b) encrypt Payment Data using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiff and the class, which would naturally result from Payment Data theft; and (e) monitor its POS systems for signs of malware to identify and mitigate any data breaches immediately.

60. Wawa permitted customers' Payment Data to be compromised by failing to take reasonable steps against an obvious threat.

61. In addition, leading up to the Data Breach, and during the course of the breach itself and the investigation that followed, Wawa failed to follow the guidelines set forth by the FTC.

62. Industry experts are clear that a data breach is indicative of data security failures. Indeed, Julie Conroy—research director at the research and advisory firm Aite Group—has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[10]

---

[9]*See, e.g.*, "Business and Credit Card Convenience Fees," THE BALANCE, https://www.thebalance.com/can-businesses-charge-a-credit-card-convenience-fee-4155333 ("Businesses that routinely accept credit cards typically build the cost of the accepting cards into their prices."); *see also* "New Rules on Electronic Payments Lower Costs for Retailers," FED. TRADE COMM'N (Sept. 2011), https://www.ftc.gov/tips-advice/business-center/guidance/new-rules-electronic-payments-lower-costs-retailers (discussing payment card fees).

[10]Lisa Baertlein, "Chipotle Says Hackers Hit Most Restaurants in Data Breach," REUTERS (May 26, 2017),

63. The Data Breach is particularly egregious and Wawa's data security failures are particularly alarming given that the breach resulted in potentially millions of cards being stolen and illegally placed for sale on the dark web. Further, the sheer length of time the Data Breach was permitted to go on for, over nine months. Clearly, had Wawa utilized adequate data security and data breach precautions, the window of the Data Breach would have been significantly mitigated, and the level of impact could have been reduced, had the breach been permitted to happen at all in the first place.

64. One commentator in the data security industry noted as to a previous, unrelated data breach:

> . . . ***2 million cards on sale on the dark web would indicate this was a very successful project for the cybercriminals involved, and one which is likely to be incredibly profitable***. POS-malware breaches happen in the US with alarming regularity, and businesses should be well aware that they need to not only protect their central networks but also need to account for physical locations as well. . . . Moving forward, financial institutions should consider implementing a system of two-factor authentication in conjunction with a passive biometric solutions in order to mitigate the entirely avoidable outcomes of security incidents such as this.[11]

65. With Payment Data stolen from potentially 850 locations over a nine-month period, this Data Breach clearly marks a highly successful outing for criminals and an exceptionally poor showing for Wawa's data security.

66. As a result of the events detailed herein, Plaintiff and members of the class suffered actual palpable fraud and losses resulting from the Data Breach, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Wawa that Plaintiff and class members

---

http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

[11]"Cyber Attack on Earl Enterprises (Planet Hollywood)," is Buzznews (Apr. 1, 2019), https://www.informationsecuritybuzz.com/expert-comments/cyber-attack-on-earl-enterprises- planet-hollywood/.

would not have made had they known of Wawa's careless approach to cybersecurity; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Data.

67. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

68. For example, the Payment Data stolen from Wawa's locations can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less- secure websites.

CLASS ALLEGATIONS

69. Plaintiff brings this action individually and on behalf of the following class pursuant to FED. R. CIV. P. 23:

> Nationwide Class: All individuals in the United States who had their credit or debit Payment Data compromised as a result of the Wawa, Inc. data breach between March 4, 2019 and December 12, 2019.

70. Excluded from the class are Wawa, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiff reserve the right to modify, change, or expand the definitions of the class based on discovery and further investigation.

71. Alternatively, Plaintiff proposes subclasses by state or groups of materially similar states, defined as follows:

> Statewide [name of State] Class: All individuals in the State(s) of [Name of State(s)] who had their credit or debit Payment Data compromised as a result of the Wawa, Inc. data breach between March 4, 2019 and December 12, 2019.

72. **Numerosity**: While the precise number of class members has not yet been

determined, members of the class are so numerous that their individual joinder is impracticable, as the proposed class appears to include members who are geographically dispersed across multiple states. Upon information and belief, the Data Breach affected millions of consumers across the United States.

73. **Typicality**: Plaintiff's claims are typical of the claims of the class. Plaintiff and all members of the class were injured through Wawa's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other class member because Plaintiff and each member of the class had their sensitive data and Payment Data compromised in the same way by the same conduct by Wawa.

74. **Adequacy**: Plaintiff is an adequate representative of the class because Plaintiff's interests do not conflict with the interests of the class that they seek to represent; Plaintiff has retained counsel competent and highly experienced in class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the class will be fairly and adequately protected by Plaintiff and her counsel.

75. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the class individually to effectively redress Wawa's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and

provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

Existence and Predominance of Common Questions of Fact and Law:

76. Common questions of law and fact exist as to Plaintiff and all members of the class. These questions predominate over the questions affecting individual class members. These common legal and factual questions include, but are not limited to, the following:

- whether Wawa engaged in the wrongful conduct alleged herein;
- whether Wawa owed a duty to Plaintiff and members of the class to adequately protect their Payment Data, and whether it breached this duty;
- whether Wawa violated federal and state laws thereby breaching its duties to Plaintiff and the class as a result of the Data Breach;
- whether Wawa knew or should have known that its computer and network systems were vulnerable to attacks from hackers and cyber criminals;
- whether Wawa's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems resulting in the theft of customers' Payment Data;
- whether Wawa wrongfully failed to inform Plaintiff and members of the class that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard consumers' sensitive financial and personal data;
- whether Wawa breached an implied contract to use industry best practices and to comply with FTC guidance to protect Plaintiff and the class's Payment Data;
- whether Wawa breached the implied covenant of good faith and fair dealing in its

contracts with Plaintiff and the class;

- whether Wawa continues to breach duties to Plaintiff and the class;
- whether Wawa has sufficiently addressed, remedied, or protected Plaintiff and class members following the Data Breach and has taken adequate preventive and precautionary measures to ensure the Plaintiff and class members will not experience further harm;
- whether Plaintiff and members of the class suffered injury as a proximate result of Wawa's conduct or failure to act; and
- whether Plaintiff and the class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the class.

77. Wawa has acted or refused to act on grounds generally applicable to Plaintiff and the other members of the class, thereby making appropriate final injunctive relief and declaratory relief with respect to the class as a whole.

78. Given that Wawa has engaged in a common course of conduct as to Plaintiff and the class, similar or identical injuries and common law and statutory violations are involved and common questions far outweigh any potential individual questions.

79. The class is defined in terms of objective characteristics and common transactional facts; namely, the exposure of sensitive Payment Data to cyber criminals due to Wawa's failure to protect this information, adequately warn the class that it lacked adequate data security measures, and failure to adequately warn that it was breached. Class membership will be readily ascertainable from Wawa's business records.

80. Plaintiff reserves the right to revise the above class definitions and any of the

averments of fact herein based on facts adduced in discovery.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

81. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

82. Wawa collected Payment Data from Plaintiff and class members in exchange for its sale of goods and other services at its impacted locations.

83. Wawa owed a duty to Plaintiff and the class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in Wawa's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Wawa's networks and data security systems to ensure that Plaintiff's and class members' financial and personal information in Hy- Vee's possession was adequately protected in the process of collection and following collection while stored on Wawa's systems.

84. Wawa further owed a duty to Plaintiff and class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

85. Wawa owed a duty to Plaintiff and class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiff and class members whose confidential data Wawa obtained and maintained.

86. Wawa knew, or should have known, of the risks inherent in collecting and storing

the financial and personal information of Plaintiff and class members and of the critical importance of providing adequate security for that information.

87. Wawa's conduct created a foreseeable risk of harm to Plaintiff and members of the class. This conduct included but was not limited to Wawa's failure to take the steps and opportunities to prevent and stop the Data Breach as described herein. Wawa's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiff and class members.

88. Wawa knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Wawa knew or should have known that hackers would attempt or were attempting to access the personal financial information in databases such as Wawa's.

89. Wawa breached the duties it owed to Plaintiff and members of the class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiff and members of the class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiff and class members.

90. As a direct and proximate result of Wawa's negligent conduct, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class)

91. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

92. Pursuant to the FTC Act, 15 U.S.C. § 45, Wawa had a duty to provide fair and

adequate computer systems and data security practices to safeguard Plaintiff's and class members' personal information.

93. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Wawa, of failing to use reasonable measures to protect Payment Data. The FTC publications and orders described above also form part of the basis of Wawa's duty to protect Plaintiff's and class members' sensitive information.

94. Wawa violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Wawa's conduct was particularly unreasonable given the nature and amount of Payment Data it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers and financial institutions.

95. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the class.

96. Wawa had a duty to Plaintiff and class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and class members' personal information.

97. Wawa breached its duties to Plaintiff and class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and

data security practices to safeguard Plaintiff's and class members' financial and personal information.

98. Wawa's violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

99. But for Wawa's wrongful and negligent breach of its duties owed to Plaintiff and class members, they would not have been injured.

100. The injury and harm suffered by Plaintiff and class members was the reasonably foreseeable result of Wawa's breach of its duties. Wawa knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and class members to suffer the foreseeable harms associated with the exposure of their Payment Data.

101. Had Plaintiff and class members known that Wawa did and does not adequately protect customer Payment Data, they would not have made purchases at Wawa's locations.

102. As a direct and proximate result of Wawa's negligence *per se*, Plaintiff and class members have suffered harm, including but not limited to loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Wawa that Plaintiff and class members would not have made had they known of Wawa's careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Data, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

103. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

104. Plaintiff and class members who made purchases at Wawa's locations during the period in which the Data Breach occurred had implied contracts with Wawa.

105. Specifically, Plaintiff and class members paid money to Wawa and, in connection with those transactions, provided Wawa with their Payment Data. In exchange, Wawa agreed, among other things: (1) to provide gasoline and other goods and services to Plaintiff and class members at its various locations; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and class members' Card Information; and (3) to protect Plaintiff's and class members' personal information in compliance with federal and state laws and regulations and industry standards.

106. Through privacy policies, codes of conduct, company security practices, and other conduct, including statements such as "Protecting your privacy is important to Wawa" and "Wawa is fully committed to data security," Wawa implicitly promised to safeguard Plaintiff's and the Class members' Payment Data in exchange for their purchases.

107. Protection of personal information was a material term of the implied contracts between Plaintiff and class members, on the one hand, and Wawa, on the other hand. Indeed, as described above, Wawa recognized the importance of data security and privacy of customers' sensitive financial information in the privacy policy. Had Plaintiff and class members known that Wawa would not adequately protect customer Payment Data, they would not have made purchases at Wawa's locations.

108. Wawa did not satisfy its promises and obligations to Plaintiff and class members under the implied contracts because it did not take reasonable measures to keep their personal information secure and confidential and did not comply with the applicable laws, regulations, and

industry standards.

109. Wawa materially breached its implied contracts with Plaintiff and class members by failing to implement adequate payment card and Payment Data security measures.

110. Plaintiff and class members fully performed their obligations under their implied contracts with Wawa.

111. Wawa's failure to satisfy its obligations led directly to the successful intrusion of Wawa's computer servers and stored Payment Data and led directly to unauthorized parties access and exfiltration of Plaintiff's and class members' Payment Data.

112. Wawa breached these implied contracts as a result of its failure to implement security measures.

113. Also, as a result of Wawa's failure to implement the security measures, Plaintiff and class members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

114. Accordingly, Plaintiff and class members have been injured as a proximate result of Wawa's breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Violation of the Pennsylvania Unfair Trade Practices Act
73 PA. STAT. ANN. § 201-1, *et seq.*
(On Behalf of Plaintiff and the Class)

115. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

116. Plaintiff and the Class purchased goods from Defendant in "trade" and "commerce" as defined in 73 Pa. Stat. Ann. § 201-2 for personal, family, and/or household purposes.

117. Defendant engaged in unlawful, unfair, and deceptive acts and practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods purchased by Plaintiff and the Class in violation of 73 Pa. Stat. Ann. §§ 201-2 and -3, including but not limited to the following:

a. Defendant misrepresented material facts pertaining to the sale of goods to Plaintiff and the Class by representing that Defendant would maintain adequate data privacy and security practices and procedures to safeguard the Payment Data of the Class from unauthorized disclosure, release, data breach, and theft, in violation of 73 Pa. Stat. Ann. § 201-2(4)(v), (ix), and (xxi).

b. Defendant misrepresented material facts pertaining to the sale of goods to Plaintiff and the Class by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Class's Payment Data, in violation of 73 Pa. Stat. Ann. § 201-2(4)(v), (ix), and (xxi).

c. Defendant omitted, suppressed, and concealed the material fact of the inadequacy of the privacy and security protections for the Class's Payment Data, in violation of in violation of 73 Pa. Stat. Ann. § 201-2(4)(v), (ix), and (xxi).

d. Defendant engaged in unfair, unlawful, and deceptive acts and practices with respect to the sale of medical supplies by failing to maintain the privacy and security of the Class's Payment Data, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws, including the FTCA, 15 U.S.C. § 45 and implementing guidance and regulations.

e. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of goods by failing to discover the Data Breach and notify the Class about it in a timely manner; and

f. Defendant engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale of goods by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect the Class's Payment Data from further unauthorized disclosure, release, data breach, and theft.

118. Further, Pennsylvania courts look to decisions interpreting the FTCA, 15 U.S.C. § 45(a) for guidance and interpretation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law. *Commonwealth by Shapiro v. Golden Gate Nat'l Senior Care LLC*, 194 A.3d 1010, 1024 n.7 (Pa. 2018).

119. As discussed above, the FTC and courts interpreting the FTCA have concluded the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3d Cir. 2015); *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

120. Defendant's failure to employ reasonable and appropriate measures, including widely followed industry practices such as point-to-point encryption or the requirements of the PCI DSS, and its continued acceptance of Plaintiff's and the Class members' payment cards, constituted an unfair or deceptive trade practice, in violation of 73 Pa. Stat. Ann. §§ 201-2(4)(v), (ix), and (xxi), and 201-3.

121. The above unlawful, unfair, and deceptive acts and practices by Defendant were unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that

the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

122. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class's Payment Data and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named deceptive acts and practices were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Class.

123. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and Class members suffered an ascertainable loss of money or property, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their Payment Data.

124. Plaintiff and The Class seek relief under 73 Pa. Cons. Stat. § 201-9.2, including injunctive relief, actual damages or $100 per Class member, whichever greater, treble damages, and attorney fees and costs.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

125. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

126. This claim is plead in the alternative to the above implied contract claim.

127. Plaintiff and class members conferred a monetary benefit upon Wawa in the form of monies paid for the purchase of goods and services at its locations.

128. Wawa appreciated or had knowledge of the benefits conferred upon them by Plaintiff and class members. Wawa also benefited from the receipt of Plaintiff's and class members' Payment Data, as this was utilized by Wawa to facilitate payment to it.

129. The monies for goods, gasoline, and other related services that Plaintiff and class members paid to Wawa were supposed to be used by Wawa, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

130. As a result of Wawa's conduct, Plaintiff and class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiff and class members paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

131. Under principals of equity and good conscience, Wawa should not be permitted to retain the money belonging to Plaintiff and class members because Wawa failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

132. Wawa should be compelled to disgorge into a common fund for the benefit of Plaintiff and class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff Linda Newton, on behalf of herself and all others similarly situated, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a) and (b)(3), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiff as class representative and her counsel as class counsel.

B. Award Plaintiff and the class appropriate monetary relief, including actual, treble, and/or statutory damages, restitution, and disgorgement.

C. Award Plaintiff and the class equitable, injunctive and declaratory relief as may be appropriate. Plaintiff, on behalf of the class, seek appropriate injunctive relief designed to protect against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly class members who are more susceptible to fraud and identity theft.

D. Award Plaintiff and the class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiff and the class reasonable attorney fees, costs, and expenses.

F. Any other favorable relief as allowable under law or at equity.

Dated: December 26, 2019

Respectfully submitted,

/s/ Benjamin F. Johns

Benjamin F. Johns
Mark B. DeSanto
Andrew W. Ferich
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
mbd@chimicles.com
awf@chimicles.com

Attorneys for Plaintiff

William B. Federman,
Pro Hac Vice application to be filed
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com